2007 Risk Assessment Project

Department of Administrative Services
Information Security Office
June 29, 2007

Project Scope

- Development of a tool for the high-level assessment of information security risks within State of Iowa agencies
- Using the tool, developed and performed a high-level risk assessments of each agency participating in the ISO Utility

Purpose of Assessments

- Gain understanding of the state of external and internal information security programs
- Make informed decisions and investments to appropriately mitigate information security risks while allowing agencies to meet or exceed service delivery obligations

Risk Assessment Tool

- Based on ISO Standard 27001:2005
- Questionnaire based:
  - Includes questions about Agency projects, applications, business processes, and service deliveries
  - Includes questions about the types of confidential information held by the Agency and how it is received, processed and transmitted
  - 93 questions used to assess risk
  - Standard set of risk descriptions and mitigation recommendations developed

Additional Tools Developed

- Checklist for conducting physical inspection/walk-through
- Pre-filled questionnaire for Agencies that use DAS/ITE for the majority of their IT support
- Standardized out-briefing with results and recommendations
- Metrics and tracking tools

Assessment Process

- Interview Agency personnel using the questions in the tool (2-3 hrs per agency)
- Review Agency answers and assign a level of risk (High, Medium, Low, Acceptable, or Not Rated) based upon risk definitions and the value of the assets requiring protection (2-4 hrs per agency)
- Prepare standardized out-briefing presentation (0.5 hrs per agency)
- Out-brief Agency and provide copy of report and presentation (0.5-1.5 hrs per agency)
- Record data in metrics spreadsheet (0.5 hr)
- Total time required per agency: 5-8.5 hrs per agency

Definition

- ***Risk***: The probable level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of its occurrence.

Ratings

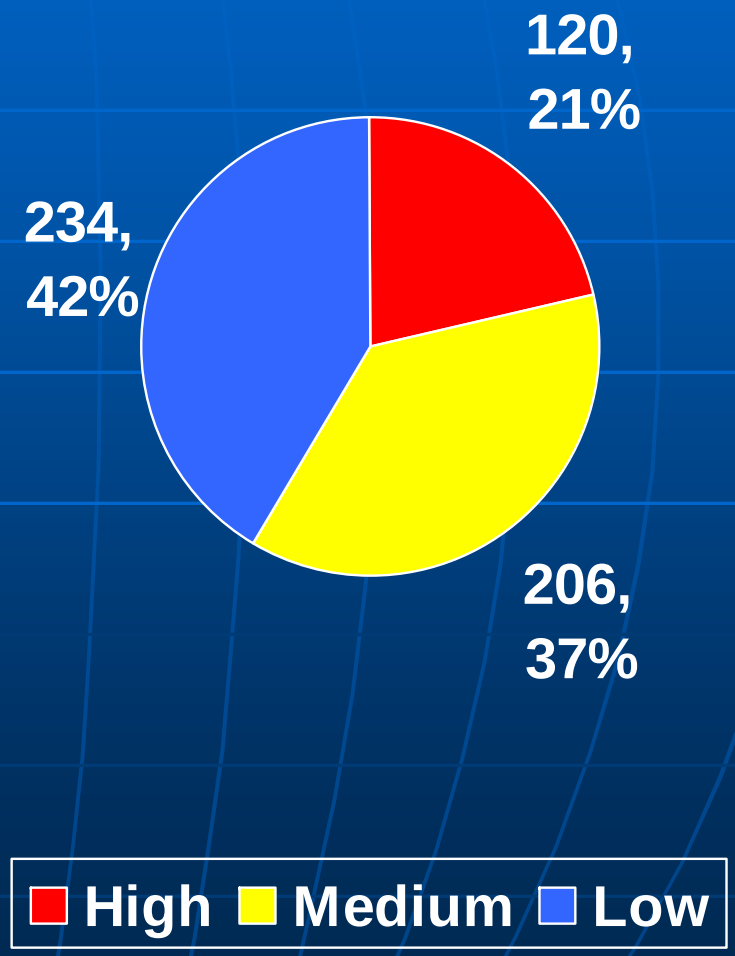
- **High Risk**: Presents significant risk to confidentiality, integrity or availability of Agency or customer data, Agency business process or service delivery obligations, and/or is likely noncompliant with statutory, regulatory or contractual requirements, based on documentation and information obtained from Agency or external sources.

- **Medium Risk**: Presents identifiable risk to confidentiality, integrity or availability of Agency or customer data, Agency business process or service delivery obligations, and/or is noncompliant with Agency policies, standards, procedures and practices, based on documentation and information obtained from Agency or external sources.

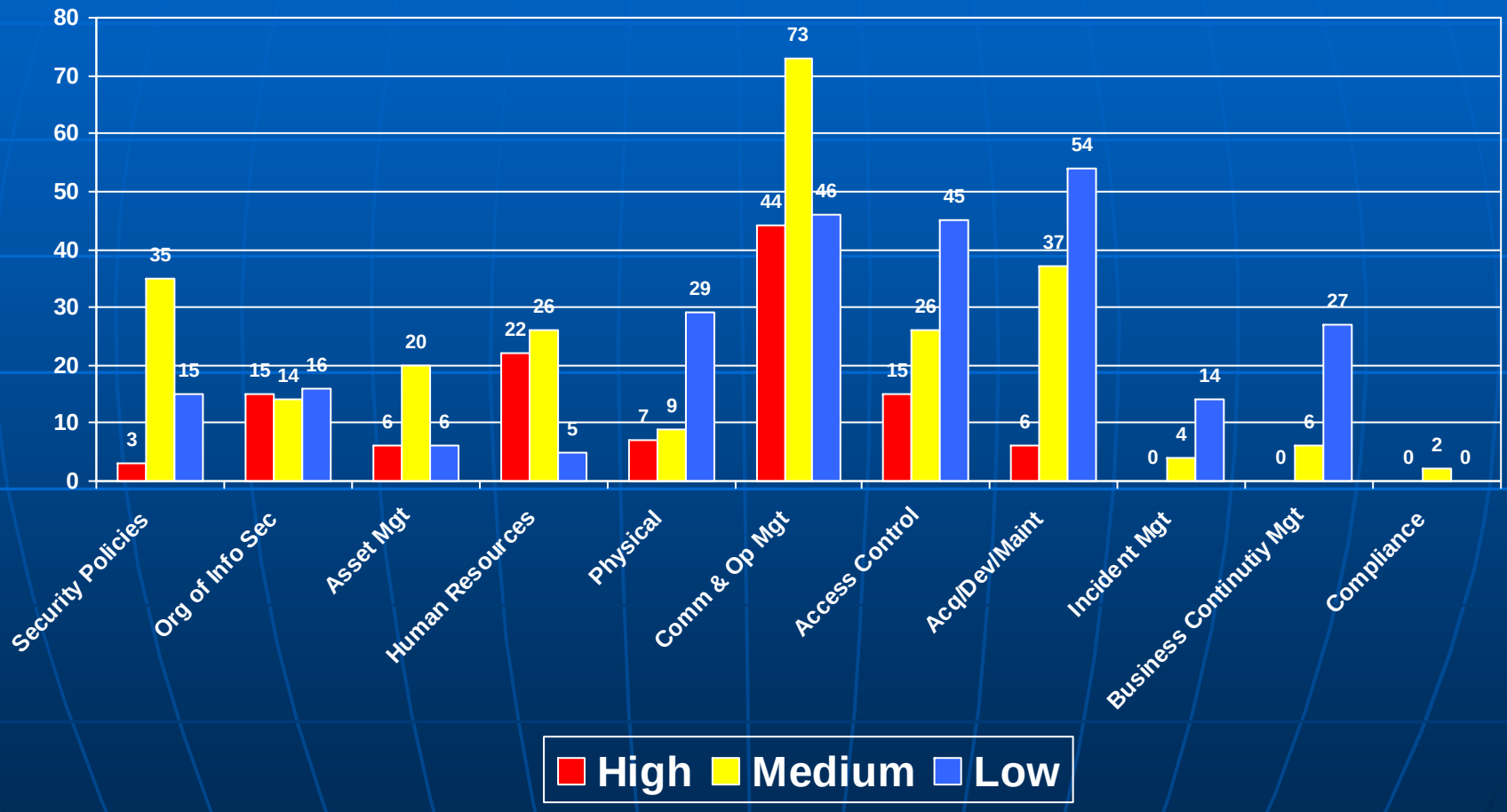
- **Low Risk**: Does not meet ISO 27001:2005 information security best practices for maintaining confidentiality, integrity or availability of Agency or customer data, Agency business process or service delivery obligations, based on documentation and information obtained from Agency or external sources.

Results

- 45 Agencies Assessed
- Total Risks Identified: 560

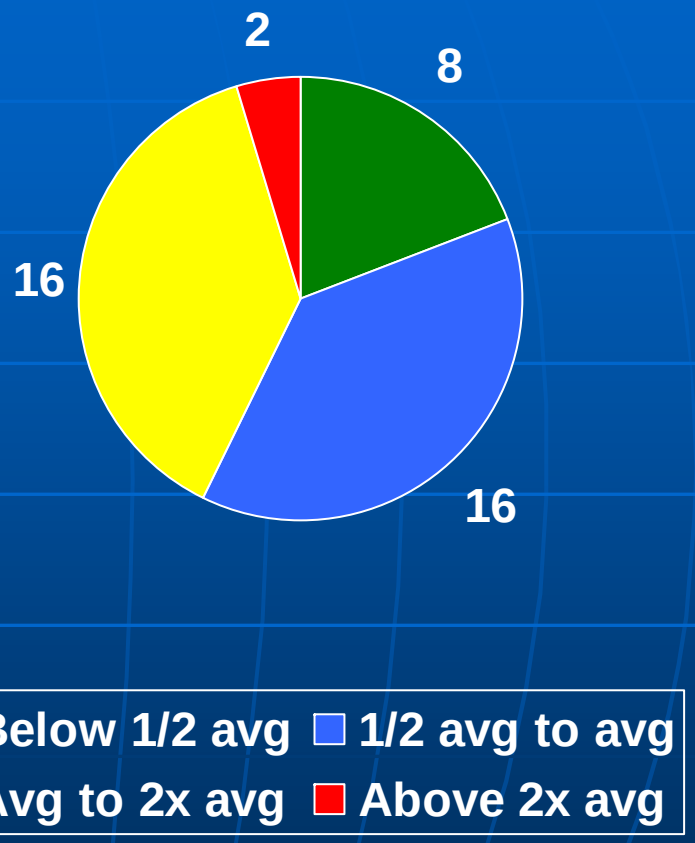


Risks by ISO Category



Agency Results

- Weighted* score based on risk level
  - Scoring range = 0-744
  - High risk = 8 points
  - Medium risk = 4 points
  - Low risk = 2 points
  - Not rated** = 1 point
- Average weighted agency score = 61.86
- Best score: 10
- Worst score: 160



* Agencies relying on DAS/ITE for the majority of IT support assume some of the DAS/ITE risks

** Where risk was noted due to lack of a control, related risks relying on the lack of the same control were not rated

Top 10 Concerns

1. Protection of log information, administrator & operator logs
2. Employment screening
3. Confidentiality agreements
4. Policy topics
5. Information classification guidelines
6. Change management
7. Encryption of mobile devices
8. Awareness, education & training
9. Segregation of duties
10. Testing, maintaining & re-assessing business continuity plans

Next 10 Concerns

11. Message Integrity
12. Ongoing External Vulnerability and Penetration Testing
13. Monitoring System Use
14. Management of Removable Media
15. OS Hardening
16. Independent Review of Information Security
17. Terms and Conditions of Employment
18. IDS/IPS Solutions
19. Physical Entry Controls
20. Clear Desk Policy

Recommendations

1. Develop an Enterprise Standard describing minimum necessary protections for all information, administrator, and operator logs and assist agencies with implementation
2. Develop an Enterprise Guideline for screening new employees
3. Develop a sample confidentiality policy and agreement and make it available to all agencies
4. Develop a policy library with sample policies on all ISO recommended topics and provide access to all agencies
5. Develop an Enterprise Guideline for information classification

Recommendations (continued)

6. Develop a set of Enterprise change management guidelines
7. Implement mobile device encryption
8. Develop Enterprise guidelines for education, awareness and training programs and continue to provide educational materials to agencies
9. Develop Enterprise guidelines for separation of duties
10. Develop an Enterprise Standard for testing of Business Continuity/COOP-COG plans

General Observations

- Physical Security
  - Excessively vulnerable – despite the need to serve the public, there are methods which can be used to partition off areas to which the public does not require access
  - Smaller outlying offices are a concern because often IT infrastructure in these areas is not protected to the same extent as central offices

General Observations (continued)

- Business Continuity Planning
  - All agencies have a COOP-COG plan
  - This is a good start – but many of the COOP-COG plans do not contain all required elements of a true Disaster Recovery and/or Business Continuity Plan
  - Most agencies haven't tested their plan or have only tested a portion of their plan

Some Next Steps

- ISO meeting with each agency to assist with planning to address risk
- Collaboration in the development of tools, templates, standards, etc. as needed by agencies
- The risk assessment process will be repeated each year to measure progress in reducing risk

Questions?